IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	**)**	
	)	**Crim. No. 18-CR-407**
v.	**)**	
	)	
ALEKSANDR BROVKO,	**)**	**Hon. T.S. Ellis, III**
	)	**Sentencing: October 23, 2020**
Defendant.	**)**	

DEFENDANT'S POSITION ON SENTENCING FACTORS

This is a case in which the calculated guideline range substantially overstates the warranted sentence – as demonstrated by the sentence imposed by this Court for Mr. Brovko's co-conspirator, Alexander Tverdokhlebov, as well as sentences imposed by this Court in similar cyberfraud cases. That is not to say that Mr. Brovko's conduct was not serious. It was serious, and he has never wavered in accepting responsibility for his wrongdoing. From his first contact with investigators (in the Czech Republic, where he has lived since 2011), Mr. Brovko admitted his role in the cyberfraud scheme at issue. He was "retained" by Tverdokhlebov, a high-level cybercriminal, and others like him to assist in cyberfraud schemes to defraud U.S. banks by hacking into customer accounts. Mr. Brovko's role was to sift through stolen user data for the personal identifying information that would allow Tverdokhlebov and others to steal money from users' bank accounts, and to further facilitate that process. For Tverdokhlebov, the mastermind of such cyberfraud schemes, this Court imposed a sentence of 110 months in 2017. *See U.S. v. Tverdokhlebov*, 1:17-CR-09, ECF Doc. 61(TSE). Similarly, in a more recent case involving an unrelated sophisticated cyberfraud scheme, this Court sentenced the organizer of that global

enterprise, Alexsei Burkov, to 108 months of imprisonment. *See U.S. v. Burkov*, 1:15-CR-245 (TSE), ECF Doc. 53.

With these cases and sentences as a guidepost, Mr. Brovko respectfully submits that a sentence of 72 months is sufficient but not greater than necessary in this case. Such a sentence reflects the seriousness of Mr. Brovko's conduct and the greater harm of the scheme in which he participated, while also taking into account the nature of his role and his personal gains relative to scheme organizers such as Tverdokhlebov and Burkov.

I. The Advisory Sentencing Guideline Range

The Probation Office has calculated the advisory guideline range in this case as 235-293 months. Mr. Brovko does not object to the Probation Office's calculated guideline range, but submits that certain guideline enhancements, as addressed below, should not be relied upon as an equitable matter in determining the appropriate sentence for Mr. Brovko.

A. Use of Special Skill – U.S.S.G. § 3B1.3

The defense raised an objection with the Probation Office regarding its application of a 2-level enhancement under § 3B1.3 for "use of a special skill" on equitable grounds. As a point of clarification, Mr. Brovko does not dispute the relatively sophisticated nature of his cyber-related knowledge and skills, but submits that his skills are no more "special" or sophisticated than those of defendant Tverdokhlebov, who did not receive this 2-level enhancement. In this regard, Mr. Brovko concedes the factual basis for the enhancement, but challenges its fairness as applied to him. Mr. Brovko acknowledges that this argument is best presented as an argument under § 3553(a), as opposed to an objection to the sentencing guidelines.

B. Loss Amount Determination

The advisory guideline range in this case is driven by the loss amount enhancement – 24 levels – which, in turn, is based not on the actual loss involved and certainly not on the gain to Mr. Brovko, but on the number of text files found on Mr. Brovko's computers at the time of his arrest. Mr. Brovko does not object to the loss amount determination under the guidelines. Indeed, the guidelines are clear as to how to calculate loss in a case such as this: number of stolen access devices (defined broadly to include any personal identification number) multiplied by $500/device. *See* U.S.S.G. § 2B1.1, Application Note 3(F)(i). Here, that formula translates into a loss amount of between $65 - $125 million.

The loss enhancement applied to Mr. Brovko is excessive and arbitrary and should not be given much weight. As far as the sentencing guidelines are concerned, the Sentencing Commission offers no empirical data to support the guidelines' $500 per access device formula, or, indeed, the loss table in general. For its part, the Sentencing Commission acknowledges that loss amount enhancements may be problematic in certain cases, and that "[t]here may be cases in which the offense level determined under this guideline substantially overstates the seriousness of the offense." U.S.S.G. § 2B1.1, Application Note 21(C). This is such a case.

Here, the loss amount determination applied to Mr. Brovko is especially arbitrary and draconian when considering that Tverdokhlebov, a higher level participant, was assessed a lower loss amount (by 4 levels) because he, Tverdokhlebov, happened to have a smaller amount of stolen data on his computers at the time of his arrest. *See* Govt. Sent. Memo. in *Tverdokhlebov*, 1:17-CR-9, ECF Doc. 54, at 5. Since loss was not measured for either defendant in terms of actual loss, the advisory guideline ranges calculated for each defendant are of little value in

assessing relative culpability. Tverdokhlebov's guideline range was calculated at 97 to 121 months, more than 50% lower than Mr. Brovko's range.

National statistics further demonstrate that a sentence at or anywhere near the advisory range in this case would be a stark outlier among § 2B1.1 offenses generally. For Fiscal Year 2019, the Sentencing Commission reported that the average sentence in fraud cases across the country was 22 months, with an average sentence of 18 months for offenders in Criminal History Category I, to 40 months for offenders in Criminal History Category VI. *See* U.S. Sentencing Commission, 2019 Sourcebook of Federal Sentencing Statistics, at Table 27.[1] Of the approximately 6,400 fraud, theft and embezzlement cases in FY 2019, the average loss amount was $6.2 million. *See* U.S. Sentencing Commission, FY 2019 Overview of Federal Criminal Cases at 20.[2]

As this Court well knows, the advisory guidelines are only one of several factors for the Court to consider under 18 U.S.C. § 3553(a). In light of the arbitrary nature of the advisory guideline calculation for Mr. Brovko, as well as national data on fraud sentencing, a significant departure from the loss enhancement-driven guideline range is called for in this case.

II. A Sentence of 72 Months Is Warranted Under the § 3553(a) Sentencing Factors

After *United States v. Booker*, sentencing is no longer a mathematical exercise. The sentencing guideline range is now advisory, and courts must consider the recommended sentencing range as one of seven statutory sentencing factors enumerated in 18 U.S.C. § 3553(a).

[1] Available at https://www.ussc.gov/sites/default/files/pdf/research-and-publications/annual-reports-and-sourcebooks/2019/Table27.pdf (last accessed Oct. 16, 2020).

[2] Available at https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2020/FY19_Overview_Federal_Criminal_Cases.pdf (last accessed Oct. 16, 2020).

Booker, 543 U.S. 220, 259-60 (2005); *see also Kimbrough v. United States*, 552 U.S. 85 (2007) (sentencing guidelines are simply an advisory tool to be considered alongside other statutory considerations set forth in 18 U.S.C. § 3553(a)); *Gall v. United States*, 552 U.S. 38 (2007) (same). After *Booker, Kimbrough* and *Gall*, therefore, sentencing courts must adhere to the primary directive of §3553(a) to "impose a sentence sufficient, but *not greater than necessary*, to comply with the purposes" of sentencing. This requirement is not just another factor to be considered along with the others set forth in Section 3553(a); rather it sets an independent limit on the sentence.

A. Personal History & Characteristics of Aleksandr Brovko

Aleksandr Brovko, now 36 years old, was born and raised in Bratsk, Russia, a city in the Siberian region of the country. He grew up with his parents and two older siblings in what he has described as a middle class household by Russian standards, equivalent to a working class background in the United States. The family lived in a small apartment, and his parents both worked. PSR, ¶¶ 51, 53. Mr. Brovko appears to have been gifted academically. After completing secondary school, he went on to the state university in Bratsk, where he eventually earned a degree in Systems Engineering in 2006. PSR, ¶ 59.

While attending the university, Mr. Brovko moved out of his family apartment to live with his girlfriend who would later become his wife. These new living expenses meant that he had to find employment, and he put the completion of his degree on hold when he found an engineering job at a local printing and advertising business. PSR, ¶ 61; letter of A. Brovko, attached as Exhibit 1. He lost that job, however, after a disagreement with the company's management. *See* Ex. 1.

While Mr. Brovko was later able to finish his coursework and earn his degree, he found that the degree did not open doors to employment opportunities as he had hoped it would. As he explains in his letter to the Court, his efforts to find legitimate employment in Bratsk were not fruitful, "either due to my lack of knowledge, or specificity of Russian business – when it is not the service quality that counts, but the number of people you know." Brovko Letter, Ex. 1.

Mr. Brovko's struggle to find employment in Russia provides the context for how he became involved in cyberfraud. His first foray into internet-based work was for a classmate who was looking for help in directing internet traffic to certain websites. Through that experience, he gained skills and professional connections, which then led him into the world of cyberfraud. It was not a path that he ever wished for, and it is one that he had hoped to resist by finding decent paying employment from legitimate sources. *See* Brovko Letter, Ex. 1.

Then, he and his wife experienced personal tragedy. As described in her letter to the Court, attached as Exhibit 2, they had a baby, a son, who died at 1 month old due to errors made by medical professionals at the local hospital. It was an extremely painful time in their lives. Mr. Brovko remains uncomfortable discussing their loss. After their first son's death, Mr. Brovko and his wife decided to move to the Czech Republic, hoping for a fresh start, and did so in 2011. There, they had a second child, also a son, who is almost 8 years old. PSR, ¶¶ 53-54.

Once settled in Ceske Budejovice, a city in the southern region of the Czech Republic, Mr. Brovko hoped to find better, legitimate employment opportunities. But moving to a new country was not the panacea he expected it to be. While he was able to learn the language, he was still seen as a foreigner in his new country.

With financial pressure mounting to provide for his family, Mr. Brovko returned to cyberfraud work which provided a steadier source of income. He was never proud of his work

and kept it secret from his wife and family. Brovko Letter, Ex. 1. His disappointment and shame in himself, in turn, exacerbated problems in his marriage. Mr. Brovko decided that it was best for his wife and son if he separated himself from their lives. Yet it is clear from his wife's letter to the Court that Mr. Brovko, his wife and their son remain a close-knit family, even after his arrest and extradition to the United States. Ex. 2, Letter of I. Brovko.

For Mr. Brovko, the most important thing in his life is his son. He recognizes and deeply regrets that his son will bear the brunt of his wrongdoing – because of his actions, his son will be without his father during his formative years.

B. Nature of The Offense

As previously described, Mr. Brovko performed a specific role in the cyberfraud schemes at issue in this case. Tverdokhlebov and others gained access to botnets – collections of computers infected by malicious software – to steal data, including personal identifying information and bank account credentials, from infected computers. Once the stolen data was collected, Mr. Brovko (and others like him) were recruited and paid to mine the data for the critical user bank account information, which Mr. Brovko passed on to co-conspirators recruited by Tverdokhlebov and others, who used the information to attempt to steal money from users' bank accounts, with Mr. Brovko's support.

Mr. Brovko was paid for his work. The government identified payments from Tverdokhlebov to Mr. Brovko totaling $137,000 in the years 2014 through 2016. While such an amount is not insignificant, it is far less than the millions that organizers like Tverdokhlebov made from the stolen data during this time. *See* Govt. Sent. Memo in *U.S. v. Tverdokhlebov*, 1:17-CR-09 (TSE), Doc. 54, at 7-8. For his part, Mr. Brovko used his earnings from cyberfraud schemes to support his wife and son, but not to live a lavish lifestyle. He also pursued legitimate

business opportunities, such as wood and food processing, but these other business ventures were not successful. PSR, ¶ 62.

On October 1, 2019, Mr. Brovko was arrested in the Czech Republic on the basis of the indictment in this case. He immediately agreed to speak to U.S. investigators who traveled to the Czech Republic for the arrest. Soon thereafter, he consented to extradition to the United States, and arrived in the Eastern District of Virginia on December 6, 2019. [3]

With his willingness to speak to investigators, his consent to extradition, and his letter to the Court, Mr. Brovko has demonstrated his acceptance of responsibility for his conduct. While there is no question that Mr. Brovko engaged in cyberfraud for several years freely and voluntarily, and was paid amply for his work, he is not someone who engaged in this fraud without a care or thought to the wrongfulness of his actions and the harm to which he contributed. He struggled with his moral failures, which he kept from his wife and family, and it seems to have been the primary cause of the dissolution of his marriage. *See* Ex. 1, Letter of A. Brovko. In short, Mr. Brovko has demonstrated that he does understand the seriousness of his wrongdoing, and has stated unequivocally that he will not return to these illegal activities once he is released to the community.

C. The Need to Avoid Unwarranted Sentencing Disparities

While the Court must consider many factors in determining the appropriate sentence in any case, the need to avoid unwarranted sentencing disparities is especially important in this case. 18 U.S.C. § 3553(a) directs the Court to consider "the need to avoid unwarranted sentence

[3] Pursuant to 18 U.S.C. § 3585(b)(1), Mr. Brovko is entitled to credit for the time that he was in custody in the Czech Republic awaiting extradition.

disparities among defendants with similar records who have been found guilty of similar conduct." *Id*. at § 3553(a)(6).

In 2017, this Court sentenced Mr. Brovko's co-conspirator, Alexander Tverdokhlebov, the "mastermind" of one or more cyberfraud schemes, to 110 months of imprisonment.[4] While Mr. Brovko no doubt played an essential role in the cyberfraud in which he participated, in relative terms, he is less culpable than organizer-leader Tverdokhlebov, who not only organized the scheme, but also, as one would expect, reaped the greatest rewards from it. Indeed, Tverdokhlebov appears to have earned millions (the government identified more than $1 million in wire transfers China and Russia before his arrest) and spent it quite lavishly, on exotic vacations and other luxury items. *See Tverdokhlebov*, 1:17-CR-09, Govt. Sent. Memo., ECF Doc. 54, at 1-2, 8. For his part, Mr. Brovko earned enough to comfortably support his family and fund his efforts to find other, legitimate business opportunities.

In *U.S. v. Burkov*, this Court sentenced another cyberfraud mastermind in June 2020 to a sentence of 108 months, effectively the same sentence it imposed on Tverdokhlebov. Burkov's guideline range was assessed at 262-327 months, for reasons similar to Mr. Brovko – a 24-level loss enhancement based on the guideline's $500-per-device formula. Notwithstanding the advisory range, and Burkov's operation of what the government called the most exclusive criminal cyberforum in the world – "a Who's Who of the world's most notorious cybercriminals,"[5] this Court's 108-month sentence reflected a substantial variance from the sentencing guidelines' recommendation.

[4] [redacted]

[5] *See Burkov*, Govt. Sent. Memo., ECF Doc. 48, at 2.

In light of his role and offense conduct, Mr. Brovko is deserving of a sentence considerably lower than defendants Tverdokhlebov and Burkov's 9 years. What Tverdokhlebov and Burkov both had, and Mr. Brovko did not, were connections to other high-level, "VIP" cybercriminals to be able to organize and operate their schemes to extract profit from stolen data. In contrast, Mr. Brovko, while his technical skills may have been considerable, played a technical role, performing work for those higher up on the cyberfraud food chain such as Tverdokhlebov and Burkov.

In sum, a sentence below the 9-year sentences imposed for Tverdokhlebov and Burkov is warranted for Mr. Brovko. In determining how far below, the sentences imposed in cyberfraud cases, *United States v. Akhalaia*, 1:18-CR-408 (TSE) (80 months), and *United States v. Yeliseyev*, 1:16-CR-310 (CMH) (72 months), are important comparisons.

In *Akhalaia*, this Court imposed a sentence of 80 months for a defendant who co-founded and operated various illicit businesses that sold stolen credit card data and personal identifying information to other cybercriminals, which earned him proceeds of between $1.5 million and $3.5 million. *See Akhalaia*, Govt. Sent. Memo, ECF Doc. 46 at 6. The amount of profit earned by Akhalaia appears more in line with Tverdokhlebov's earnings than those of Mr. Brovko. In this regard, Akhalaia's 80-month sentence supports a sentence of less than 80 months for Mr. Brovko.

Finally, in the case of *U.S. v. Yeliseyev*, the Court imposed a sentence of 72 months, later reduced to 48 months, for a cyberfraud defendant who "acted as a middleman between large-scale computer hackers and retail-level fraudsters" trafficking in stolen credit card data. *See Yeliseyev*, 1:16-CR-310, Govt. Sent. Memo., ECF Doc. 44, at 1. As in Mr. Brovko's case, the actual loss attributable to Yeliseyev was difficult to determine, and thus the $500-per-device was

applied, resulting in a loss figure of between $25 and $65 million, one level lower on the loss chart than that applied to Mr. Brovko. While it is difficult to gauge the ways in which Mr. Brovko and defendant Yeliseyev are either similar or dissimilar from the limited information available in the record, Yeliseyev's role as a "middleman" suggests a mid-level role, which could be said of Mr. Brovko as well. Mr. Brovko was not involved in deploying or organizing the massive data theft (through botnets), but played a technical and admittedly important role in extracting the valuable information from the stolen data, and paving the way for the subsequent financial theft.

When considered together, the aforementioned cyberfraud cases support a sentence of 72 months for Mr. Brovko as the sentence necessary to avoid creating any unwarranted sentencing disparity among similar and related defendants.

D. The Need to Achieve Deterrence, Promote Respect for the Law, and Impose A Sentence that Provides Just Punishment

Deterrence is a difficult concept to quantify in relation to 18 U.S.C. § 3553(a)'s mandate that the Court impose a sentence which is sufficient but not greater than necessary. Research from a variety of sources, including the Department of Justice, has concluded that increasing the severity of punishment does not, in fact, result in greater deterrence. Rather, it is the fact of prosecution which has a deterrent impact. *See* U.S. Department of Justice Office of Justice Programs, *Five Things About Deterrence* (May 2016), available at https://www.ncjrs.gov/pdffiles1/nij/247350.pdf.

Here, Mr. Brovko faces a substantial period of imprisonment, in a country where he does not speak the language, and has no personal connections. For Mr. Brovko, the experiences of arrest and extradition alone are sufficient to deter him from future criminal activity, and a lengthy sentence is not necessary in that regard. For others engaged in international cyberfraud,

arrest, extradition and imprisonment for 5 years or more sends a resounding message and is sufficient to achieve general deterrence.

III. Conclusion

As in every case, sentencing in this case requires the Court to balance myriad factors and determine the sentence that is sufficient but not greater than necessary. For the reasons set forth above, it is respectfully submitted that a sentence of 72 months is warranted and represents the sentence that is sufficient but not greater than necessary to achieve the goals of sentencing for Mr. Brovko.

Respectfully submitted,

ALEKSANDR BROVKO
By Counsel,

By: _____/s/_____

Shannon S. Quill
Virginia Bar No. 76355
Assistant Federal Public Defender
Attorney for A. Brovko
1650 King Street, Suite 500
Alexandria, Virginia 22314
(703) 600-0850 (telephone)
(703) 600-0880 (facsimile)
Shannon_Quill@fd.org (email)

CERTIFICATE OF SERVICE

I hereby certify that on the 18th day of October 2020, I will file the foregoing with the Clerk of Court using EM/ECF, which will then send a notification of such filing to the following:

Laura Fong, Esq.
Alexander Berrang, Esq.
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, VA 22314

/s/

Shannon S. Quill, Esquire
Virginia bar No. 76355
Attorney for A. Brovko
Office of the Federal Public Defender
1650 King Street, Suite 500
Alexandria, VA 22314
(703)600-0850 (telephone)
(703)600-0880 (facsimile)
shannon_quill@fd.org